De spagaat van de CISO: beheersbaarheid versus verantwoordelijkheid

In de steeds complexere digitale wereld wordt van de Chief Information Security Officer (CISO) meer verwacht dan enkel technische expertise. De CISO moet een strategische rol vervullen en de balans vinden tussen operationele controle en langetermijn-doelstellingen. Daarbij is het essentieel om draagvlak te creëren bij de directie en het senior management, bijvoorbeeld door middel van educatie en strategische communicatie. Van de CISO wordt ook verwacht dat hij of zij actief bijdraagt aan bredere bedrijfsdoelstellingen en risicobeheersing. Dit artikel bespreekt hoe de CISO deze spagaat kan overbruggen, samenwerkingsverbanden binnen de organisatie versterkt, en informatiebeveiliging positioneert als een strategisch voordeel dat niet alleen groei bevordert, maar ook voldoet aan belangrijke regelgeving.

De rol van de Chief Information Security Officer (CISO) is zowel veelzijdig als veeleisend, met als grootste uitdaging het vinden van een evenwicht tussen strategische verantwoordelijkheid en operationele controle. Afhankelijk van de organisatie kan de invulling van de functie sterk verschillen, wat de complexiteit van de rol alleen maar vergroot. De CISO is altijd verantwoordelijk voor het waarborgen van informatiebeveiliging, maar de mate waarin hij of zij betrokken is bij operationele of strategische taken, varieert aanzienlijk per organisatie.

Rol van de CISO

In sommige organisaties is de CISO nauw betrokken bij de technische uitvoering van beveiligingsmaatregelen en is sprake van een hands-on rol in operationele activiteiten. In andere gevallen werkt de CISO voornamelijk op strategisch niveau samen met het topmanagement om beleid te ontwikkelen dat de organisatie beschermt tegen een breed scala aan risico's. Vooral in grotere organisaties, met complexe IT-infrastructuren, opereert de CISO op strategisch niveau. In kleinere bedrijven is de CISO daarentegen vaak meer direct betrokken bij de praktische uitvoering van maatregelen en dagelijkse beveiligingsprocessen.

Een veelvoorkomend probleem is dat organisaties niet altijd goed inzicht hebben in de positionering van de CISO binnen hun bredere risicobeheerstructuur. Het 'Three Lines of Defense'-model kan daarbij nuttig zijn. In dit model is de eerste lijn verantwoordelijk voor de uitvoering van operationele beveiligingsmaatregelen, de tweede lijn voor toezicht en risicobeheersing, en de derde lijn voor onafhankelijke audits. Binnen dit model opereert de CISO strikt genomen vanuit een tweede lijn. Hoewel dit model een theoretisch duidelijke scheiding van verantwoordelijkheden biedt, vervagen in de praktijk deze grenzen vaak. Dit ondermijnt de effectiviteit van de CISO, die verantwoordelijk is voor strategische besluitvorming, maar beperkt wordt door een gebrek aan directe controle over de implementatie.

De rol van de CISO vereist dat zij flexibel blijft, inspelend op dreigingen en beperkte middelen en politieke uitdagingen binnen de organisatie. Budgettaire beperkingen kunnen het werk van de CISO verder bemoei-

lijken, vooral wanneer de directie kiest voor het uitstellen of afzwakken van cruciale beveiligingsmaatregelen. Dit creëert een lastige situatie waarin de CISO verantwoordelijk is voor het rapporteren van risico's die niet volledig beheersbaar zijn, omdat de benodigde middelen of het mandaat ontbreekt om adequate maatregelen te nemen.

Het spanningsveld tussen verantwoordelijkheid en beheersbaarheid creëert aanzienlijke druk op CISO's. De combinatie van hoge verwachtingen, beperkte operationele controle en de voortdurende dreiging van cyberaanvallen draagt bij aan een groeiend aantal gevallen van burn-out. Uit een Gartner-onderzoek uit 2023 bleek dat 62% van de CISO's minstens één keer met burn-out te maken heeft gehad, terwijl 44% dit meerdere keren heeft ervaren. Deze cijfers benadrukken niet alleen de intensiteit van de rol, maar ook de persoonlijke tol die het kan eisen van degenen die verantwoordelijk zijn voor de bescherming van steeds complexere digitale omgevingen.

Om de effectiviteit van de CISO te vergroten, het welzijn van de persoon in deze cruciale functie te waarborgen en de rol beter te verankeren binnen de organisatie, is het essentieel om de CISO strategisch te positioneren binnen het bredere management en risicobeheer. Dit vraagt niet alleen om een duidelijke afbakening van verantwoordelijkheden, maar ook om het toewijzen van voldoende middelen en operationele ondersteuning. De CISO is dan niet alleen verantwoordelijk voor het bepalen van de strategische richting, maar beschikt ook over middelen om deze effectief te realiseren.

Een voorbeeld hiervan is dat mijn team beveiligingsrisico's heeft vertaald naar de taal van de business, zodat de business begrijpt waarom maatregelen essentieel zijn voor het succes en continuïteit van de organisatie.

Strategieën voor succes: hoe de spagaat te overbruggen

Wanneer de rol van CISO nieuw wordt ingevoerd binnen een organisatie, biedt dit zowel kansen om informatiebeveiliging strategisch te verankeren als uitdagingen in het balanceren tussen strategische verantwoordelijkheid en operationele controle. Het opbouwen van een effectieve beveiligingsfunctie begint vaak met het ontwikkelen van meerjarige roadmaps, die de lange termijndoelen en prioriteiten vaststellen. Deze roadmaps bieden duidelijke richting en helpen de strategie af te stemmen op veranderingen in technologie, processen en medewerkers.
Als eerste CISO bij Van Oord kreeg ik de unieke kans om deze cruciale functie vanaf de grond op te bouwen. Ik ontwikkelde een driejarige roadmap, waarin ieder jaar specifieke projecten werden gerealiseerd om de weerbaarheid van de organisatie te versterken. Bij elk initiatief zorgde ik ervoor dat processen, technologie en mensen nauw op elkaar afgestemd waren.
Zo maakten we niet alleen risico's beheersbaar, maar ondersteunden we ook strategische groei en continuïteit. Deze aanpak stelde ons in staat om flexibel in te spelen op zowel groeiende dreigingen als veranderende bedrijfsprioriteiten. Bovendien zorgde de jaarlijkse realisatie van nieuwe capabilities voor vertrouwen in de roadmap en versterkte het de beveiligingspositie van de organisatie.

Een veelvoorkomende valkuil in organisaties die nog in de opstartfase zitten, is dat de CISO te veel betrokken blijft bij de operationele uitvoering van beveiligingsmaatregelen. Binnen de organisatie is de functie vaak onvoldoende strategisch gepositioneerd of beschikt over te weinig operationele ondersteuning, wat leidt tot inefficiënties en de CISO belemmert om zich effectief te richten op strategische prioriteiten.

Ook in meer volwassen organisaties blijft het een uitdaging om de CISO effectief te positioneren binnen het bredere risicomanagement, vooral wanneer de functie nog sterk operationeel is. Hoewel de CISO verantwoordelijk is voor het beheren van beveiligingsrisico's, is dit slechts één onderdeel van het grotere bedrijfsrisicobeheer. Idealiter wordt de CISO geïntegreerd in de bredere corporate risk-strategie, waarin informatiebeveiliging als een cruciale pijler fungeert. Door informatiebeveiliging op deze manier strategisch te positioneren, kan het een integraal onderdeel worden van de bredere bedrijfsdoelstellingen, in plaats van een geïsoleerd proces. In de praktijk blijft de focus van corporate risk management echter vaak beperkt tot financiële risico's, waardoor de informatiebeveiligingsfunctie onvoldoende wordt benut en de CISO niet de mogelijkheid heeft om effectief te opereren op strategisch niveau. Dit creëert een gemiste kans om informatiebeveiliging volledig te integreren als een cruciaal onderdeel van het bredere risicobeheer.

Om deze balans tussen strategische verantwoordelijkheid en operationele controle te realiseren, is het cruciaal dat bestuurders en directie actief samenwerken met de CISO om diens rol duidelijk te definiëren binnen de tweede lijn van risicobeheer. Voor CISO's is het van groot belang om proactief het gesprek aan te gaan met de directie om hun strategische positie te versterken, zodat hun rol niet alleen operationeel blijft, maar actief bijdraagt aan de algemene bedrijfsdoelstellingen.

Het creëren van een helder risico en control framework helpt om rollen en verantwoordelijkheden af te bakenen, waardoor de CISO het overzicht behoudt zonder vast te lopen in operationele details.

Bovendien is het essentieel dat de CISO verandert van een top-down controlerende functie naar een vraaggestuurde rol. Een vraaggestuurde aanpak houdt in dat beveiligingsinitiatieven worden afgestemd op de strategische prioriteiten van de organisatie en niet slechts worden opgelegd vanuit compliance-oogpunt. Dit versterkt de samenwerking tussen de beveiligingsfunctie en de business, waardoor beveiligingsmaatregelen beter aansluiten op de operationele behoeften van de organisatie.

Mijn team heeft van mij de opdracht gekregen om samen met de bedrijfsonderdelen verschillende informatiebeveiligingsdiensten te ontwikkelen die inspelen op hun specifieke behoefte. Deze benadering stimuleert een cultuur van waardecreatie, waarbij het CISO-team zich richt op het leveren van beveiligingsdiensten die bijdragen aan bedrijfscontinuïteit en winstgevende groei. Door duidelijke performance indicatoren te hanteren, zoals KPI's en SLA's, maken we de impact en waarde van onze diensten transparant en meetbaar. Dit klantgerichte model zorgt ervoor dat beveiligingsoplossingen relevant zijn voor de business en breed worden geaccepteerd. Het vermindert weerstand omdat de oplossingen zijn afgestemd op de strategische doelen van de organisatie en bijdragen aan de algehele bedrijfscontinuïteit. Hierdoor wordt beveiliging niet langer gezien als een kostenpost, maar als een strategisch voordeel. Dit stelt een CISO in staat om zich te positioneren als een onmisbare, strategische partner voor de directie.

Door deze strategische en vraaggestuurde aanpak versterkt de CISO niet alleen de controle over informatiebeveiliging, maar creëert hij ook een gezonde balans tussen verantwoordelijkheid en beheersbaarheid. Dit leidt tot een effectiever risicobeheer en draagt direct bij aan het behalen van bedrijfsdoelstellingen. Bovendien vergroot deze benadering de veerkracht van de organisatie, terwijl de persoonlijke druk op de CISO en het team wordt verminderd, wat bijdraagt aan een duurzamere en productieve werkomgeving.

De weg van verandering

Het succesvol implementeren van beveiligingsinitiatieven vraagt niet alleen om technische expertise, maar vooral om het vermogen om de directie en het senior management mee te nemen in het strategische belang van informatiebeveiliging. In veel organisaties wordt beveiliging nog te vaak gezien als een kostenpost of een operationele kwestie. De uitdaging voor de CISO is om dit gesprek te verschuiven naar de strategische waarde die beveiliging biedt op het gebied van bedrijfscontinuïteit, groei en concurrentiekracht; en daarmee de spagaat tussen operationele verantwoordelijkheden en strategische doelstellingen te overbruggen.

Wanneer de directie terughoudend is of onvoldoende zicht heeft op de kansen en risico's van informatiebeveiliging, kan educatie een krachtig middel zijn om bewustwording te vergroten. Het aanbieden van gerichte trainingen en workshops helpt om de impact van beveiliging op de bredere bedrijfsstrategie te verduidelijken. Wet- en regelgeving zoals Network and Information Security (NIS2)-richtlijn of de Artificial Intelligence (AI) Act bieden concrete ingangen om het gesprek aan te gaan. De nadruk moet liggen op de strategische implicaties van niet-naleving, zoals reputatieschade of verlies van marktaandeel. Voor multinationals is het daarbij essentieel om ook wetgeving buiten de EU in acht te nemen. De CISO speelt hier een sleutelrol door aan te geven wanneer de beveiligingsmaatregelen toereikend zijn en verdere stappen geen toegevoegde waarde meer bieden.

Het opbouwen van sterke samenwerkingsverbanden binnen de organisatie is eveneens cruciaal. Door samen te werken met afdelingen zoals compliance, legal en interne audit, kan de CISO ervoor zorgen dat informatiebeveiliging niet wordt gezien als een geïsoleerd IT-probleem, maar als een integraal onderdeel van het bredere risicomanagement en de governance-structuur van de organisatie. Dit versterkt de positionering van beveiliging op de strategische agenda en helpt de CISO om de spagaat tussen operationele betrokkenheid en strategische verantwoordelijkheid effectief te beheersen.

Het is daarnaast essentieel om beveiligingsdoelstellingen op een manier te presenteren die directie en senior management aanspreekt. In plaats van zich te richten op technische risico's en potentiële dreigingen, kan de CISO beter benadrukken hoe een robuuste beveiligingsstrategie bijdraagt aan de veerkracht en continuïteit van de organisatie. Dit helpt om beveiliging te positioneren als een strategisch voordeel in plaats van een verplichting. Tegelijkertijd blijft het belangrijk om in wederzijds vertrouwen met de directie te bepalen wanneer de beveiliging "goed genoeg" is om de risico's beheersbaar te houden zonder onnodige druk op operationele processen en budgetten.

Door educatie, samenwerking en strategische communicatie kan de CISO niet alleen informatiebeveiliging steviger verankeren binnen de organisatie, maar ook zichzelf positioneren als een betrouwbare strategische partner die directie en management ondersteunt bij het realiseren van bredere bedrijfsdoelstellingen. De CISO fungeert daarbij als een belangrijke adviseur en toezichthouder die de organisatie helpt risico's effectief te beheersen en zich voor te bereiden op toekomstige uitdagingen.

Als u dit artikel leest in uw rol als CISO en worstelt met het vinden van de juiste balans tussen operationele controle en strategische doelen, onthoud dan dat uw verantwoordelijkheid verder reikt dan het managen van beveiligingsmaatregelen. Uw waarde ligt in het vermogen om beveiliging te positioneren als een strategisch voordeel, dat direct bijdraagt aan de bredere bedrijfsdoelstellingen. Werk nauw samen met de directie, spreek hun taal, en gebruik regelgeving zoals NIS2 niet alleen om te voldoen aan de eisen, maar om uw organisatie sterker en veerkrachtiger te maken. Uiteindelijk wordt succes bepaald door uw capaciteit om beveiliging naadloos te verbinden met groei en continuïteit – en zo uw organisatie naar een hoger niveau te tillen.

Referentie

(1) https://www.gartner.com/en/articles/cybersecurity-leaders-are-burned-out-here-s-why

Auteurs: Marcel Spruit is Lector Cybersecurity aan het Kenniscentrum Cybersecurity van de Haagse Hogeschool in Den Haag. Hij is te bereiken via m.e.m.spruit@hhs.nl. Céline Kreffer was ten tijde van het onderzoek waarop deze publicatie is gebaseerd Onderzoeker Cybersecurity aan het Kenniscentrum Cybersecurity van de Haagse Hogeschool. Nu is zij Analist Bestuurlijke Informatie bij het Ministerie van Justitie en Veiligheid in Den Haag. Zij is bereikbaar via https://www.linkedin.com/in/céline-kreffer-71170212a/.